



Digital for job:

La privacy nella sanità digitale


Sergio Ferri

Sommario

Il 2017 e gli anni successivi saranno molto impegnativi per il settore sanitario perché si dovrà iniziare a implementare e rendere operative le innovazioni già approvate in ambito normativo, innovazioni che si inquadrano nel più ampio scenario della digitalizzazione della nostra Pubblica Amministrazione.

Ai riferimenti normativi emanati negli anni precedenti, come quelli relativi al Fascicolo Sanitario Elettronico (FSE), si sono aggiunti nel 2016 l'aggiornamento del Codice dell'Amministrazione Digitale (CAD), il Patto per la sanità digitale e l'approvazione del Regolamento UE del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR). Tutte norme che avranno un impatto diretto sul settore sanitario, in quanto, essendo il Servizio Sanitario Nazionale (SSN) parte integrante della Pubblica Amministrazione, ogni processo innovativo dovrà tenere conto di tutto lo scenario normativo di riferimento: SSN, CAD e del nuovo "Codice degli appalti" (quest'ultimo non trattato in questo articolo). Inoltre, essendo i dati sanitari, "dati sensibili", la normativa attuale e futura in ambito privacy deve essere considerata un requisito imprescindibile.

Le innovazioni riguarderanno principalmente i processi, e avranno successo soltanto se, come riportato nel Patto della salute digitale, ci saranno interventi formativi adeguati che possano permettere agli operatori del settore sanitario di implementare le innovazioni nel loro iter lavorativo traendone benefici e non creando invece un'inutile complessità. AICA negli ultimi anni ha sviluppato un'offerta formativa finalizzata a supportare le trasformazioni nell'ambito dell'informatica giuridica e più specificatamente nella sanità creando certificazioni e utilizzando i test center affiliati anche per erogare i corsi.



Abstract

During 2015 some relevant rules have been approved or updated: the guidelines of the “Fascicolo Sanitario Elettronico (FSE)”, the updating of the “Codice dell’Amministrazione Digitale (CAD)”, the “Patto per la sanità digitale” and the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation (GDPR).

All these rules will have a relevant impact on the “Servizio Sanitario Nazionale (SSN)” as part of the Public Administration. Consequently every innovative process shall take into account the applicable laws’ framework including: SSN, CAD and the new “Codice degli appalti” (this law has not been introduced in this article). Furthermore the sanitary data shall be managed as sensitive data therefore the privacy law requirements shall be taken into account.

Keywords: Accountability, Data controller, Data Protection Officer, ECDL, eHealth, ePrescription, GDPR, healthcare, patient summary, privacy.

1- Sanità digitale

Il Servizio Sanitario Nazionale ha una complessità molto elevata, in quanto, oltre ad un numero molto elevato di utenti e di operatori, non è costituito da un’unica amministrazione, bensì da un insieme di enti ed organi che concorrono al raggiungimento degli obiettivi di tutela della salute dei cittadini. Conseguentemente ogni innovazione deve tener conto della complessità intrinseca nel sistema.

Quindi quando si parla di “sanità digitale” si deve intendere l’insieme degli interventi condivisi da tutte le Amministrazioni operanti a livello centrale, regionale e locale per la digitalizzazione del ciclo prescrittivo, la realizzazione di una soluzione federata di Fascicolo Sanitario Elettronico (FSE) del cittadino e l’aumento del tasso di innovazione digitale nelle aziende sanitarie (**Fig.1 La sanità digitale**).

Nell’articolo saranno utilizzati molti acronimi il cui significato è riportato nel riquadro **Acronimi utilizzati**.

Acronimi utilizzati

AgID Agenzia per l’Italia Digitale
ANA Anagrafe Nazionale degli Assistiti
CAD Codice dell’Amministrazione Digitale
DPCM Decreto del Presidente del Consiglio dei Ministri
FSE Fascicolo Sanitario Elettronico
GDPR General Data Protection Regulation
MMG Medico di Medicina Generale
PLS Pediatra di Libera Scelta
SSN Servizio Sanitario Nazionale

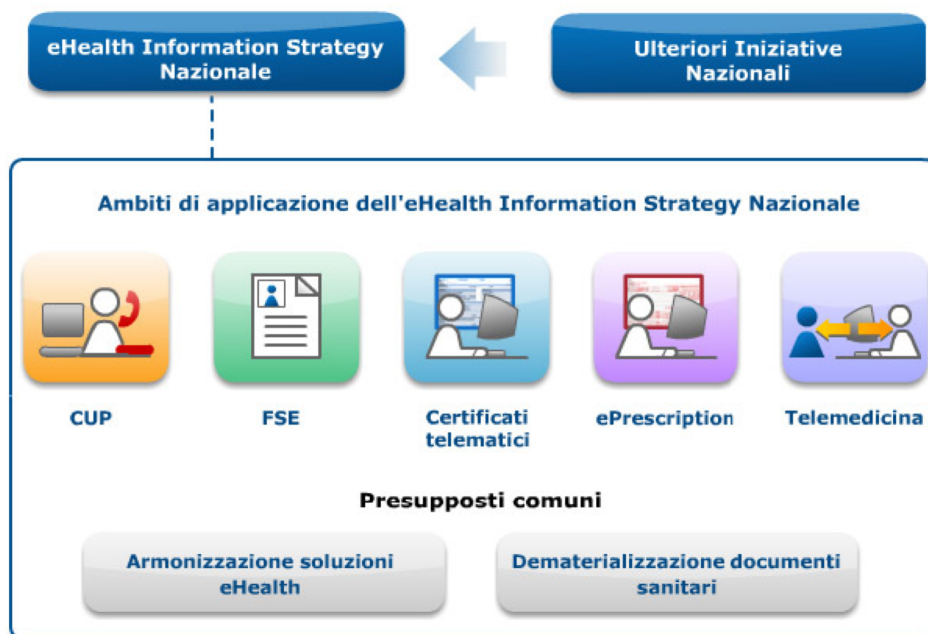


Figura 1

La sanità digitale

(Fonte: Sito del Ministero della Salute www.salute.gov.it)

1.1 Fascicolo Sanitario Elettronico FSE

Nel DPCM n.178 del 29 settembre 2015 è stato pubblicato il regolamento per il Fascicolo Sanitario Elettronico (FSE), strumento innovativo che migliora drasticamente il livello di cura dei pazienti e che si inserisce all'interno del Codice dell'Amministrazione Digitale (CAD).

Il FSE è l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti il singolo assistito. Ha un orizzonte temporale che copre l'intera vita del paziente ed è alimentato in maniera continuativa dai soggetti che lo prendono in cura nell'ambito del SSN e dei servizi socio-sanitari regionali. Il FSE è costituito, previo consenso dell'assistito, dalle Regioni e Province Autonome per le finalità di prevenzione, diagnosi, cura e riabilitazione perseguite dai soggetti del SSN e dei servizi socio-sanitari regionali che prendono in cura l'assistito.

I contenuti del FSE sono costituiti da un nucleo minimo di dati e documenti, nonché da dati e documenti integrativi che permetteranno di arricchirne il contenuto informativo. Il nucleo minimo, che deve essere eguale per tutte le regioni e province autonome italiane, contiene i fascicoli sanitari istituiti da regioni e province autonome, ed è costituito dai dati identificativi e amministrativi del singolo assistito, i referti, i verbali pronto soccorso, le lettere di dimissione il profilo sanitario sintetico, il dossier farmaceutico ed il consenso o diniego alla donazione degli organi e tessuti. Mentre i dati e documenti integrativi sono ulteriori componenti del FSE, la cui alimentazione è funzione delle scelte

regionali in materia di politica sanitaria e del livello di maturazione del processo di digitalizzazione (Fig.2 Alimentazione del Fascicolo Sanitario Elettronico)

Un elemento importante del FSE è rappresentato dal profilo sanitario sintetico, o "Patient summary", cioè il documento socio-sanitario informatico redatto e aggiornato dal Medico di Medicina Generale/Pediatra di Libera Scelta (MMG/PLS), che riassume la storia clinica dell'assistito e la sua situazione corrente conosciuta. La finalità del profilo sanitario sintetico è di favorire la continuità di cura, permettendo un rapido inquadramento dell'assistito al momento di un contatto con il SSN. Il Patient Summary è un documento elettronico di sintesi, firmato digitalmente, derivante dalla Scheda Sanitaria Individuale del paziente (prevista negli Accordi Collettivi Nazionali della medicina di base), creato e mantenuto dal MMG/PLS, il cui scopo è quello di fornire un'istantanea sul quadro clinico, demografico e amministrativo di uno specifico paziente. Attraverso il Patient Summary il MMG/PLS documenta tutti e soli i dati che ritiene rilevanti di un paziente e li rende disponibili ad altri operatori sanitari autorizzati, al fine di garantire la continuità della cura.

Il FSE deve rispondere a tutti i requisiti dei trattamenti di dati personali quali l'identificazione del titolare e dei dati del trattamento, la definizione delle finalità di accesso, il consenso e l'accesso da parte dell'assistito. Le finalità del trattamento possono essere: cura, ricerca e governo. Ovviamente il tipo di dati a cui un operatore sanitario può accedere è diverso in base alle specifiche finalità del trattamento o trattamenti a cui è autorizzato.

Il FSE deve garantire l'allineamento dei dati identificativi degli assistiti con i dati contenuti nell'Anagrafe Nazionale degli Assistiti (ANA) o, se non disponibili, nelle anagrafi sanitarie regionali, allineate con l'anagrafe nazionale della popolazione residente come specificato nel CAD.

Trattando il FSE dati sanitari, le misure di sicurezza previste sono molto stringenti. Le operazioni sui dati personali, necessarie per trattamenti previsti, devono essere effettuate utilizzando strumenti elettronici che assicurino confidenzialità, integrità e disponibilità dei dati, come previsto nel D.Lgs. 196/03 per la protezione dei dati personali e successive modificazioni, incluso l'allegato B relativo al disciplinare tecnico. Mentre la riservatezza dei dati trattati nell'ambito del FSE è garantita dalle procedure di sicurezza relative al software e ai servizi telematici utilizzati, attuate in conformità a quanto previsto dal CAD. Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati si deve operare secondo accorgimenti idonei per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi. Sono inoltre previste specifiche misure di sicurezza dei dati nella fase di consultazione.

Le modalità di accesso al FSE sono esplicitate dall'assistito attraverso due categorie di consenso:

- Consenso all'alimentazione: permette l'alimentazione del FSE da parte dei MMG/PLS e degli operatori e professionisti sanitari;

- Consenso alla consultazione: permette la consultazione dei dati e dei documenti presenti nel FSE, da parte dei MMG/PLS e degli operatori per finalità di cura, sulla base di:
 - modalità di visibilità indicate dall'assistito in base al ruolo professionale;
 - contesti operativi, quali il trattamento dati di cura ordinario e in emergenza.

Ovviamente l'assistito può essere in grado di fornire un consenso informato solo se gli operatori sanitari gli hanno fornito una quantità ed un livello di informazioni adeguate allo scopo.

Come si è potuto constatare le modalità di gestione dei trattamenti dei dati contenute nel FSE sono riprese dal Codice della privacy di cui si parlerà in seguito.

Altri elementi caratterizzanti il FSE provengono dal Codice dell'Amministrazione Digitale (c.d. CAD) che non è altro che una struttura integrata di disposizioni sviluppata per fornire indicazioni operative e standardizzate sull'utilizzo dell'informatica all'interno delle pubbliche amministrazioni e nei loro rapporti con il cittadino.

Nel CAD, entrato in vigore nel 2010, è stato aggiornato a settembre del 2016, le disposizioni che hanno un impatto più visibile per gli operatori sanitari, relativamente al FSE, riguardano le definizioni e le norme tecniche relative al documento informatico, alla firma digitale e alla trasmissione dei documenti informatici.

Il documento informatico può essere definito come la rappresentazione di contenuti testo, immagini e filmati ottenuta attraverso un processo di elaborazione elettronica: questa rappresentazione è di tipo numerico, cioè insieme di bit, che viene memorizzata in modo permanente su un supporto fisico, che può essere un disco rigido o una memoria ottica, quindi non in una memoria volatile. I vantaggi principali del documento informatico rispetto a quello cartaceo sono la drastica riduzione dell'ingombro fisico, la maggior velocità nella ricerca e nell'aggiornamento dei dati, la possibilità di utilizzo contemporaneo in uno stesso documento di elementi multimediali (quali immagini e suoni) e infine la possibilità di trasmissione a distanza in tempo reale utilizzando la rete Internet.

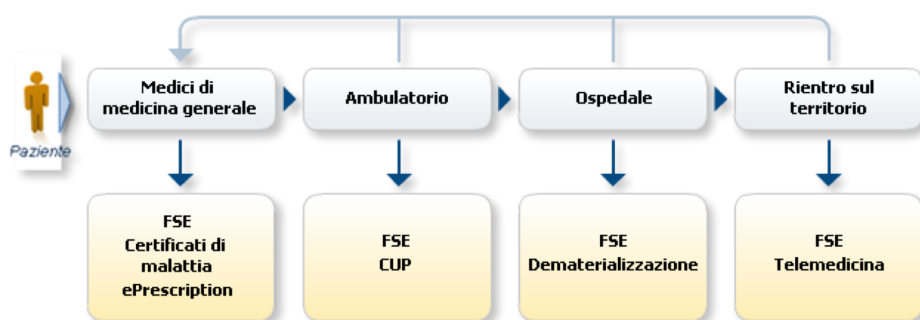


Figura 2
Alimentazione del Fascicolo Sanitario Elettronico
(Fonte: Sito del Ministero della Salute www.salute.gov.it)

A fronte di questi vantaggi intrinseci della tecnologia digitale, le norme tecniche CAD sono state sviluppate per permettere di risolvere le problematiche che impattano su un documento di cui qui di seguito si riporta solo un accenno. Il documento informatico deve contenere un metodo efficace di autenticazione che ne eviti le manipolazioni, essere in un formato portabile nei diversi sistemi informatici, utilizzare una trasmissione sicura e un sistema di conservazione che possa garantire l'autenticità della sua eventuale riproduzione.

Le norme tecniche del CAD sono state inserite nel "Disciplinare tecnico" allegato alle sopra menzionate Linee guida del FSE per far fronte ai requisiti di questa particolare tipologia di documento. Conseguentemente le regioni e le province autonome dovranno utilizzare uno specifico sistema di classificazione e codifica dei dati. Il "Sistema di classificazione" ripartisce gli oggetti dati in classi o raggruppamenti ordinandoli in base ad un principio di ordinamento, mentre il "Sistema di codifica" assegna un identificativo univoco (alfabetico, numerico o alfanumerico) a ciascun oggetto di un dato insieme.

Al fine di garantire la privacy i dati anagrafici non sono inseriti all'interno del FSE, ma sono gestiti in archivi separati alimentati dall'Anagrafe Nazionale degli Assistiti (ANA) e, dove questa non è disponibile, sono alimentati dalle anagrafi sanitarie regionali. Sempre per rispettare la privacy devono essere definiti e gestiti profili di accesso per le classi di dati identificate: anagrafici, amministrativi, prescrittivi, clinici e di consenso del cittadino.

La conservazione dei documenti informatici di tipo sanitario e socio-sanitario deve essere effettuata ai sensi del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 – "Regole tecniche in materia di conservazione di documenti informatici". I soggetti del SSN e dei servizi socio-sanitari regionali che prendono in cura l'assistito e che producono i dati e i documenti sanitari utilizzati per alimentare il FSE, sono titolari del trattamento dei dati e dei documenti informatici e responsabili della loro conservazione. Il processo di conservazione può essere affidato, in modo totale o parziale, a conservatori pubblici o privati, che offrano adeguate garanzie organizzative e tecnologiche e previo accreditamento presso l'Agenzia per l'Italia Digitale

1.2 Patto per la sanità digitale

Il Patto per la sanità digitale, sottoscritto dal ministero per la Salute il 23 settembre 2016, è il piano strategico unitario e condiviso per il conseguimento degli obiettivi di efficienza, trasparenza e sostenibilità del SSN, attraverso l'impiego sistematico dell'innovazione digitale in sanità. Le priorità di intervento che faranno parte del patto sono riconducibili a logiche di *performance based contracting* in ambiti dove l'efficientamento dei processi di erogazione dei servizi possa garantire significative economie gestionali. Queste priorità verranno discusse *in progress* in modo da giungere a una versione condivisa con tutti gli stakeholders.

Lo scopo è la promozione sistematica dell'innovazione digitale utilizzando i fondi disponibili. La governance sarà attuata tramite un Comitato di Coordinamento del Patto, formato da un rappresentante per ciascuna delle categorie di stakeholder coinvolte. Per ognuna delle priorità progettuali individuate potrà

essere costituito un gruppo di lavoro specifico, partecipato da tutti gli stakeholder interessati ed esteso – su chiamata specifica – alla partecipazione di consulenti e ricercatori esterni.

Il primo elenco di priorità inserite nel piano è riportato nel riquadro: **Patto digitale per la salute, primo elenco delle priorità.**

Patto per la sanità digitale

Estratto dal Documento programmatico

- Modelli organizzativi e strumenti per la razionalizzazione dell'infrastruttura IT della Sanità Pubblica; business continuity e disaster recovery;
- Unified Communication e Collaboration come nuova modalità di interazione multidisciplinare tra professionisti in ambito ospedaliero e territoriale;
- Soluzioni e servizi per la continuità assistenziale ospedale-territorio: i PDTA come nuova modalità di approccio e i sistemi di Patient Workflow Management;
- Dal "Taccuino personale del cittadino" al "Personal Healthcare Assistant": nuove piattaforme di servizi "information intensive" per i cittadini. Dalla prenotazione e check-in on line, dal pagamento multicanale e contactless al download e upload bidirezionale di informazioni sullo stato di wellness;
- Cure primarie: nuovi modelli organizzativi e cartella clinica condivisa;
- Sistemi Informativi Ospedalieri integrati;
- Modelli e soluzioni per la Clinical Governance;
- Logistica del farmaco, "farmaco a casa" e Soluzioni di Business Intelligence per il monitoraggio dell'appropriatezza delle prescrizioni farmaceutiche;
- Teleconsulto, teleriferazione, tediagnosi, telemonitoraggio, teleriabilitazione; telemedicina e integrazione col Fascicolo Sanitario Elettronico;
- Analisi e condivisione sull'utilizzo di "SNOMED CT" quale standard semantico di riferimento per lo scambio di informazioni di salute relative ai cittadini a livello nazionale e transfrontaliero; valutazione dell'impatto derivante dall'adozione di tale standard.

1

0

2. La normativa privacy

Nel 1996 venne emanata in Italia la prima normativa estensiva sulla privacy, successivamente nel 2003 è entrato in vigore il c.d. Testo Unico della Privacy: Decreto Legislativo 30 giugno 2003, n. 196, "*Codice in materia di protezione dei dati personali*", attualmente in vigore.

Mentre il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea è stato pubblicato il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), c.d. GDPR (General Data Protection Regulation), che come previsto nell'art. 99 è entrato in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale (25 maggio 2016), ma si applicherà a decorrere dal 25 maggio 2018. A questa data le leggi nazionali sulla privacy dei paesi membri dell'unione europea decadranno.

1

0

2.1 Il D.Lgs. 196/03 Codice privacy

Questo decreto legge è denominato “*Codice in materia di dati personali*”, il titolo chiarisce in modo univoco le sue finalità cioè che la protezione della privacy si deve basare sulla protezione dei dati dei singoli individui. Quindi la legge ha definito all’articolo 4 quali caratteristiche hanno i dati personali, cosa si deve intendere per trattamento e in particolare i ruoli e le responsabilità di coloro che possono trattare i dati personali. Come si può vedere nel riquadro – Definizioni (art.4 del D.Lgs.196/03) dove sono riportate le singole definizioni estratte dal art. 4 della legge, i dati sanitari rientrano nella categoria dei dati sensibili. Nello stesso riquadro si ritrovano le definizioni dei termini menzionati in precedenza nella normativa sul Fascicolo Sanitario Elettronico.

L’impianto generale della legge, gli articoli da 75 a 94, dedicati ai *Trattamenti di dati personali in ambito sanitario* e le successive Autorizzazioni generali emesse dall’Autorità garante hanno un livello descrittivo e prescrittivo tale che hanno permesso alle diverse tipologie di strutture sanitarie di impostare un proprio Sistema documentale ed organizzativo di Gestione della Privacy (SGP).

Nelle “*Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*” l’Autorità garante aveva evidenziato alcune problematiche relative alla privacy dei pazienti che sono state successivamente inserite nel DPCM n.178 del 2015 descritto in precedenza, a conferma della sinergia fra le differenti istituzioni che sovrintendono, in base alle loro specifiche competenze e ruoli, le innovazioni organizzative nell’ambito del SSN.

Definizioni (art. 4 del D.Lgs. 196/03)

“trattamento”, qualunque operazione o complesso di operazioni, effettuati anche senza l’ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

“dato personale”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

“dati sensibili”, i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare **lo stato di salute** e la vita sessuale;

“titolare”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

"responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **"interessato"**, la persona fisica cui si riferiscono i dati personali:

2.2 Regolamento Europeo

Il *Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* che sostituirà la normativa nazionale, è in realtà l'equivalente di una nostra legge delega, che secondo il nostro ordinamento è una legge che delega il Parlamento ad esercitare la funzione legislativa su una determinata tematica. In questo caso al fine di conseguire gli obiettivi del Regolamento, il Parlamento europeo ha delegato la Commissione ad adottare gli atti delegati riguardanti specifici atti di esecuzione, quali norme tecniche e meccanismi di certificazione, misure specifiche per piccole e medie imprese e clausole contrattuali tipo tra responsabili e titolari del trattamento.

Il Regolamento introduce alcune novità, quelle che avranno un maggiore impatto nel settore sanitario sono: i principi di trasparenza e accountability, la Privacy by Design e l'introduzione del ruolo di Data Privacy Officer che sarà obbligatorio per tutte le pubbliche amministrazioni e per le organizzazioni che trattano prevalentemente dati personali, come nel caso del settore sanitario. Per la descrizione di queste e delle altre innovazioni che dovranno essere operative a decorrere dal 25 maggio 2018 si rimanda alla lettura del Regolamento europeo.

3. La formazione AICA per la sanità digitale

3.1 AICA per la sanità

AICA da oltre cinquant'anni è punto di riferimento per la costruzione della società digitale. Da alcuni anni ha avviato diverse iniziative e realizzato pubblicazioni volte a valutare gli impatti delle nuove tecnologie dell'informazione e della comunicazione sul mondo della sanità e a qualificare, valorizzandole, le competenze ICT degli operatori sanitari. Nel 2016 ha promosso un Osservatorio delle competenze digitali in sanità e gestisce una serie di certificazioni che hanno l'obiettivo di formare gli operatori nelle competenze necessarie per essere attori proattivi nei processi di trasformazione del settore e del proprio modo di lavorare.

3.2 L'Osservatorio delle Competenze Digitali in Sanità 2016

Nel contesto della Sanità Digitale si evidenzia la necessità di promuovere la cultura della sanità elettronica con programmi di formazione specifici da attuarsi sia nell'ambito del corso di studi e master universitari che all'interno della

Educazione Continua in Medicina (ECM), processo attraverso il quale il professionista della salute si mantiene aggiornato per rispondere ai bisogni dei pazienti, alle esigenze del Servizio Sanitario e al proprio sviluppo professionale.

AICA ha deciso quindi di promuovere, con l'appoggio e il sostegno del Ministero della Salute, Direzione Generale della Digitalizzazione, del Sistema Informativo Sanitario e della Statistica, l'Osservatorio sulle Competenze Digitali in Sanità in Italia, che ha coinvolto Associazioni mediche di settore, professionisti della Sanità, ordini professionali, Università e istituzioni interessate al tema.

L'obiettivo è stato quello di analizzare e verificare - tramite confronto soprattutto con le Professioni Sanitarie e con qualificati operatori del settore - lo stato dell'arte e le diverse tipologie di competenze e i conseguenti percorsi di formazione richiesti per le diverse figure coinvolte nel processo - differenziabili tra competenze digitali di base per tutti gli Utenti, competenze digitali specialistiche per gli Addetti ai lavori e competenze di e-leadership - intese come capacità di utilizzare al meglio le tecnologie digitali all'interno di qualsiasi tipo di organizzazione e di introdurre innovazione digitale nello specifico settore di mercato in cui si opera. I risultati dell'Osservatorio sono stati presentati presso il Ministero della salute il 26 settembre 2016, la versione integrale del rapporto finale è disponibile sul portale AICA.

Dai risultati della ricerca si evince la necessità di condivisione anche strategica a livello nazionale su "criteri minimi" e di indirizzo per l'utilizzo della sanità digitale anche se è stato evidenziato uno scarso coinvolgimento del personale sanitario nei progetti di informatizzazione, con sviluppi che di conseguenza rischiano di non rispettare le specifiche esigenze del reparto e/o del servizio. Inoltre si è evidenziata una forte sensibilità da parte di medici e infermieri rispetto al trattamento dei dati sanitari, ma non si sono rilevate competenze adeguate rispetto alla conoscenza del codice della privacy e delle misure di sicurezza necessarie per la protezione dei dati sanitari. Altri ambiti in cui la richiesta di formazione è maggiore sono le conoscenze relative alle applicazioni del Sistema Sanitario Nazionale, al Fascicolo Sanitario Elettronico e alla Telemedicina. Significativa è anche la richiesta di formazione per l'uso di risorse informative avanzate come le banche dati ed i servizi cloud. Purtroppo emerge anche che la formazione e l'aggiornamento continuo sulle competenze digitali in sanità hanno una distribuzione non sempre omogenea nelle nostre Università e nelle Aziende Sanitarie o IRCCS.

3.3 Formazione per la sanità

Aica è presente già da tempo con un'offerta per il settore sanitario. Nel 2008 è stata annunciata la certificazione Ecdl Health, destinata ai medici, agli infermieri, ai tecnici che utilizzano il computer nell'attività quotidiana. Questa certificazione, nata dalle specifiche di un gruppo di esperti europei, è stata successivamente aggiornata e l'ultimo aggiornamento (il cui Syllabus è stato pubblicato anche nelle linee guida per le competenze dell'Agenzia Digitale) deriva dal lavoro congiunto di un gruppo di professionisti del settore, appartenenti ad Associazioni, Ordini medici, Società di formazione medica. Nel 2015 è stato accreditata da Accredia come certificazione professionale per gli operatori della

sanità e, in quanto certificazione a carattere professionale, è stata chiamata eHealth, mentre Ecdl Health rimane come percorso di formazione certificato per le scuole (Istituti Socio Sanitari). Come materiale didattico di supporto alla certificazione è disponibile anche un corso learning con crediti ECM.

La certificazione HealthDoc, sviluppata in collaborazione con l'Istituto Superiore della Sanità e l'Associazione Bibliotecari e documentaristi in Sanità, intende verificare le competenze di chi ricerca informazioni e documentazione scientifica.

Sono in fase di definizione le competenze di eleadership specifiche per il settore, che non riguardano professionisti ICT, ma quelle figure che devono saper rendere più efficaci i processi e i prodotti aziendali grazie all'utilizzo delle nuove tecnologie. A questo progetto sta lavorando, oltre ad AICA, un gruppo di professionisti sanitari e la Fondazione Politecnico di Milano. In questo ambito è stato condotto un percorso di assessment delle competenze di CIO associati ad Associazione Italiana Sistemi Informativi in Sanità (AISIS) - rispetto allo standard e-CF (european Competence Framework)- per definire i percorsi di formazione più allineati alle effettive necessità. Corsi sviluppati da SDA Bocconi.

Attraverso il **programma di certificazione "Informatica Giuridica"**, AICA propone uno strumento di definizione delle conoscenze necessarie, di verifica delle competenze e di certificazione delle abilità acquisite, riguardanti l'informatica giuridica e le implicazioni legali e formali nell'utilizzo di tecnologia ICT. Le competenze riguardano, tra le altre, la normativa CAD e gli strumenti quali la Posta Elettronica Certificata (PEC) e la Firma Digitale.

Nel primo quadrimestre di quest'anno è prevista la disponibilità di una certificazione Privacy per i professionisti che operano nelle strutture sanitarie. La certificazione richiederà le conoscenze e le competenze necessarie per rispettare la normativa privacy nello svolgimento delle attività di cura utilizzando gli strumenti della sanità digitale, quali il sopra descritto Fascicolo Sanitario Elettronico. Questa certificazione è supportata da un libro scritto da esperti del settore.

Al fine di fornire una comprensione migliore dell'offerta formativa AICA per il settore sanitario, si riporta di seguito la **Tabella 1** che la riassume.

Settore	Denominazione	Descrizione
SANITARIO	eHealth	Strumenti della sanità digitale, certificazione per i professionisti della sanità.
	ECDL Health	Strumenti della sanità digitale, certificazione per gli Istituti Socio Sanitari.
	HealthDoc	Informazione documentale e scientifica
	Privacy in sanità (Disponibilità prevista: 1°2017)	La normativa privacy applicata alle strutture sanitarie

Settore	Denominazione	Descrizione
INFORMATICA GIURIDICA	Protezione Dati Personali Privacy e Sicurezza	Evoluzione del concetto di privacy e la relativa normativa italiana
	Firma Digitale e Posta Elettronica Certificata	Conoscenza e utilizzo della Firma Digitale e della Posta Elettronica Certificata
	e-Governance e Amministrazione Digitale	Il Codice dell'Amministrazione Digitale (CAD)
	Gestione Documentale e dematerializzazione	Caratteristiche e peculiarità del documento informatico come definito dal Codice dell'Amministrazione Digitale.
MANAGEMENT	eCF (european Competence Framework)	CIO in sanità 23 profili professionali informatici
	ePMQ (european Project Management Qualification)	Competenze del Project manager

Bibliografia e Sitografia

- [1] G. Mastronardi, S. Ferri, *Sanità digitale e privacy*, Edizioni Manna, 2017
- [2] www.agid.gov.it/agenda-digitale/pubblica-amministrazione/sanita-digitale
- [3] www.agid.gov.it/tags/fascicolo-sanitario-elettronico
- [4] www.aicanet.it (ultimo accesso 23 gennaio 2017)
- [5] garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 (ultimo accesso 23 gennaio 2017)
- [6] www.salute.gov.it (ultimo accesso 23 gennaio 2017)

Biografia

Sergio Ferri è consulente privacy in Beamat. Ha un'esperienza trentennale nei sistemi organizzativi e nelle infrastrutture IT con requisiti di elevata sicurezza. Negli ultimi anni svolge servizi di consulenza per la progettazione e l'implementazione di Sistemi di Gestione della Privacy. E' docente a contratto nei corsi di Privacy e Sicurezza IT per AICA, per la Scuola IAD della Università Roma 2 e per società di formazione. Ha partecipato a studi e progetti in ambito sanitario, ha ricoperto il ruolo di esperto privacy nell'"Osservatorio Competenze Digitali in Sanità 2016" promosso da AICA.

email: sergio.ferri@beamat.it